APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,776	11/15/2001	Esa Turtiainen	032986-019	4500

27045   7590   09/19/2005

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR C11
PLANO, TX 75024

EXAMINER
GELAGAY, SHEWAYE

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 09/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	10/003,776	TURTIAINEN ET AL.
	Examiner	Art Unit	
	Shewaye Gelagay	2133	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>28 July 2005</u>.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-7</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-7</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   This office action is in response to Applicant's amendment filed on July 28, 2005.

Claims 1, 3-5 and 7 have been amended. Claims 1-7 are pending.

Specification

2.   In view of the amendment filed July 28, 2005, the Examiner withdraws the

objection to the specification.

Claim Rejections - 35 USC § 112

3.   In view of the amendment filed July 28, 2005, the Examiner withdraws the

rejection of claims 3 and 4 under 35 U.S.C. 112.

Response to Arguments

4.   Applicant's arguments with respect to claims 1-7 have been considered but are

moot in view of the new ground(s) of rejection. In response to the arguments concerning

the previously rejected claims, the following comments are made:

In response to applicant's argument that the references fail to show certain

features of applicant's invention, it is noted that the features upon which applicant relies

(i.e., using only the IKE component to negotiate a IPSec SA data relevant to the

encryption) are not recited in the rejected claim(s). Although the claims are interpreted

in light of the specification, limitations from the specification are not read into the claims.

See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The Applicant argues Mamros et al. (hereinafter Mamros, U.S. Patent 6,360269)

does not disclose "sending a datagram without IPSec headers". The Examiner

disagrees. Mamros discloses a protected link is formed between the first node and the

second node and all traffic channels are encrypted. (Col. 5, lines 64-67) Once the

secured link has been established, the first node and the second node are able to

communicate securely. (Col. 6, lines 17-23) The messages between the two nodes do

not contain IPSec headers because the IPSec data is confined to link 213 and channel

203. (see Figure 2) Therefore, Mamros anticipates datagram not including IPSec

header or headers.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed
> or described as set forth in section 102 of this title, if the differences between the
> subject matter sought to be patented and the prior art are such that the subject
> matter as a whole would have been obvious at the time the invention was made
> to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was
> made.

This application currently names joint inventors. In considering patentability of

the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of

the various claims was commonly owned at the time any inventions covered therein

were made absent any evidence to the contrary. Applicant is advised of the obligation

under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was

not commonly owned at the time a later invention was made in order for the examiner to

consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g)

prior art under 35 U.S.C. 103(a).

6.   Claims 1 and 3-7 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Mamros et al. (hereinafter Mamros) United States Letter Patent Number 6,360,269

in view of Patel et al. IP Security Working Group, Internet Draft, Intel Corporation

(hereinafter Patel).

As per claim 1:

Mamros teach a method of sending streamed data over an IP network from a first

node to a second node, the method comprising:

using Internet Key Exchange (IKE) to establish an IKE security association (SA)

between the first and second nodes; (Col. 6, lines 9-13)

passing the IKE SA data to streamed data applications associated with the

streamed data; (Col. 5, lines 63-67; Col. 6, lines 1-5 and lines 14-22; *IKE is interpreted*

as ISAKMP. The interpretation is giving based on the description given on the

disclosure. Page 6)

encrypting the streamed data at the first node with a cipher using a shared secret

forming part of said IPSec SA; (Col. 6, lines 2-3)

constructing IP datagrams containing the encrypted streamed data, the

datagrams not including an IPSec header or headers; (Col. 5, lines 51-67 and Col. 6,

lines 1-7) and

sending the IP datagrams from the first node to the second node. (Col. 2, lines

44-45; Col. 3, lines 15-30 and lines 45-47)

In addition, Mamros discloses sending encrypted streamed data. (Col. 1, lines

66-67 and Col. 2, line 1; Col. 6, line 2). Furthermore, Mamros disclose establishing

secure and authenticated channel using ISAKMP/Oakley protocol. (Col. 6, lines 8-22)

Mamros does not explicitly disclose using phase 1 negotiation to establish

security association between the first node and second nodes and phase 2 negotiations

for each transmission direction.

Patel in analogous art, however, discloses using phase 1 negotiation to establish

security association (SA) between the first node and second nodes (Page 1, paragraph

5; Page 2, paragraph 1) phase 2 negotiations for each transmission direction. (Page 1,

paragraph 5; page 2, paragraph 1)

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify the device disclosed by Mamros to include

using phase 1 negotiation to establish security association between the first node and

second nodes and phase 2 negotiations for each transmission direction. This

modification would have been obvious because a person having ordinary skill in the art

would have been motivated to do so, as suggested by, Patel (Page 2, paragraph 2) in

order to reduce a startup time for communication and improve the efficiency of the

protocol.

As per claim 3:

Mamros and Patel teach all the subject matter as discussed above. In addition,

Mamros further discloses a method wherein said first and second nodes are end points

for the data. (Figure 1; Col. 3, lines 27-29)

As per claim 4:

Mamros and Patel teach all the subject matter as discussed above. In addition,

Mamros further discloses a method wherein said first and second nodes tunnel data

between respective end points. (Figure 2; Col. 3, lines 27-29)

As per claim 5:

Mamros teaches an apparatus for securing streamed data over an IP network

from a first node to a second node, the apparatus comprising:

processing means and memory containing software instructions for implementing

IPSec protocols; (Fig 3, items 303, 305; Col. 6, lines 9-13)

an application for delivering streamed data; (Col. 2, lines 44-45; Col. 3, lines 15-

30 and lines 45-47)

means for using Internet Key Exchange (IKE) to establish an IKE security

association (SA) between the first and second nodes; (Col. 5, lines 63-67; Col. 6, lines

1-5 and lines 14-22)

means for passing the IPSec SA data to applications associated with the

streamed data; (Col. 5, lines 63-67; Col. 6, lines 1-5 and lines 14-22)

encrypting means for encrypting the streamed data at the first node with a cipher using the shared secret forming part of said IPSec SA; (Col. 6, lines 2-3)

means for constructing IP datagrams containing the encrypted streamed data, the datagrams not including an IPSec header or headers; (Col. 5, lines 51-67 and Col. 6, lines 1-7) and

transmission means for sending the IP datagrams from the first node to the second node. (Col. 2, lines 44-45; Col. 3, lines 15-30 and lines 45-47)

In addition, Mamros discloses sending encrypted streamed data. (Col. 1, lines 66-67 and Col. 2, line 1; Col. 6, line 2). Furthermore, Mamros disclose establishing secure and authenticated channel using ISAKMP/Oakley protocol. (Col. 6, lines 8-22)

Mamros does not explicitly disclose using phase 1 negotiation to establish security association between the first node and second nodes and phase 2 negotiations for each transmission direction.

Patel in analogous art, however, discloses using phase 1 negotiation to establish security association (SA) between the first node and second nodes (Page 1, paragraph 5; Page 2, paragraph 1) phase 2 negotiations for each transmission direction. (Page 1, paragraph 5; page 2, paragraph 1)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Mamros to include using phase 1 negotiation to establish security association between the first node and second nodes and phase 2 negotiations for each transmission direction. This modification would have been obvious because a person having ordinary skill in the art

would have been motivated to do so, as suggested by, Patel (Page 2, paragraph 2) in

order to reduce a startup time for communication and improve the efficiency of the

protocol.

As per claim 6:

Mamros and Patel teach all the subject matter as discussed above. In addition,

Mamros further discloses an apparatus, the apparatus being an end user terminal such

as a telephone, communicator, PDA or palmtop computer, or a personal computer (PC).

(Figure 2; Col. 3, line 15)

As per claim 7:

Mamros and Patel teach all the subject matter as discussed above. In addition,

Mamros further discloses an apparatus, the apparatus being a firewall or gateway

coupled to the first node which is the source of the streamed data. (Figure 2; Col. 3, line

23)

7.   Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mamros

et al. (hereinafter Mamros) United States Letter Patent Number 6,360,269 in view of

Patel et al. IP Security Working Group, Internet Draft, Intel Corporation (hereinafter

Patel) further in view of Rao et al. (hereinafter Rao) United States Letter Patent Number

6,757,823.

As per claim 2:

Mamros and Patel teach all the subject matter as discussed above. Both

references do not explicitly disclose a method wherein said streamed data is VoIP data

or videoconferencing data.

Rao in analogous art, however, discloses a method wherein said streamed data

is VoIP data or videoconferencing data. (Col. 4, lines 12-18)

Therefore, it would have been obvious to a person having ordinary skill in the art

at the time the invention was made to modify the device disclosed by Mamros and Patel

to include a method wherein said streamed data is VoIP data or videoconferencing

data. This modification would have been obvious because a person having ordinary skill

in the art would have been motivated to do so, as suggested by, Rao (Col. 1, lines 7-9)

in order to provide enhanced security for Internet telephony calls and secure connection

for VoIP.

Conclusion

8.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure. See Form PTO-892.

Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay
09/12//05

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100